Sub a1

What is claimed is:

1. A method for authenticating transmitted data in real time, the method comprising the steps of:

(a) generating a master cryptographic key pair, including a first public key and a first private key;

(b) publishing a first certificate issued by a certificate authority, the first certificate including the first public key and a first digital signature based on the first public key;

(c) generating a disposable cryptographic key pair, including a second public key and second private key;

(d) generating a second certificate, the second certificate including the second public key and a second digital signature based on the second public key;

(e) publishing the second certificate;

(f) signing the data to be transmitted with a third digital signature by processing the data through a one way hashing function to generate a first hash value and encrypting the first hash value utilizing the second private key;

(g) processing the received data through the one way hashing function to create a second hash value;

(h) decrypting the received third digital signature utilizing the second public key to obtain a third hash value; and

(i) verifying the authenticity of the data by comparing the second hash value to the third hash value.

2. The method for authenticating transmitted data in real time according to claim 1, wherein the step of generating a master key pair comprises creating long first public and private keys.

3. The method for authenticating transmitted data in real time according to claim 1, wherein the first certificate further includes the identification of the sender and the identification of the certificate authority issuing the first certificate.

4. The method for authenticating transmitted data in real time according to claim 3, wherein the first digital signature is produced by:

(a) processing the data representing the identification of the sender, the identification of the certificate authority and the first public key through a one way hashing function to create a fourth hash value; and

(b) encrypting the fourth hash value utilizing a private key from the certificate authority to create the first digital signature.

5. The method for authenticating transmitted data in real time according to claim 4, further comprising the step of verifying the authenticity of the data comprising the first certificate.

6. The method for authenticating transmitted data in real time according to claim 5, wherein the step of verifying the authenticity of the data comprising the first certificate comprises:

(a) decrypting the first digital signature to obtain a fifth hash value utilizing a public key issued by the certificate authority;

(b) processing the received data representing the identification of the sender, the identification of the certificate authority and the first public key through a one way hashing function to create a sixth hash value; and

(c) comparing the fifth and sixth hash values.

7. The method for authenticating transmitted data in real time according to claim 1, wherein the step of generating a disposable cryptographic key pair comprises generating short second public and private keys.

8. The method for authenticating transmitted data in real time according to claim 1, wherein the second certificate further includes the identification of the sender and the identification of the signing authority issuing the second certificate.

9. The method for authenticating transmitted data in real time according to claim 8, wherein the second digital signature is produced by:

(a) processing the data representing the identification of the sender, the identification of the signing authority and the second public key through a one way hashing function to create a seventh hash value; and

(b) encrypting the seventh hash value utilizing the first private key to create the second digital signature.

10. The method for authenticating transmitted data in real time according to claim 9, further comprises the step of verifying the authenticity of the data comprising the second certificate.

11. The method for authenticating transmitted data in real time according to claim 10, wherein the step of verifying the authenticity of the data comprising the second certificate comprises:

(a) decrypting the second digital signature to obtain an eighth hash value utilizing the first public key;

(b) processing the received data representing the identification of the sender, the identification of the signing authority and the second public key through a one way hashing function to create a ninth hash value; and

(c) comparing the eighth and ninth hash values.

12. The method for authenticating transmitted data in real time according to claim 1, further comprises dividing the data into packets and signing and authenticating each packet of data in accordance with steps (f) through (i) of claim 1.

13. A method for digitally signing data in real time, the method comprising the steps of:

(a) generating a master key pair including a first public key and a first private key;

(b) publishing a first certificate, the first certificate including the first public key and a first digital signature based on a certificate authority's key pair;

(c) generating a disposable key pair, the disposable key pair including a second public key and a second private key, and wherein the disposable key pair is shorter than the master key pair;

(d) generating a second certificate, the second certificate including the second public key and a second digital signature based on the master key pair;

(e) dividing the data to be signed into packets;

(f) for each packet of data, computing a hash value based on the data in that data packet utilizing a one way hashing function;

(g) encrypting the hash value utilizing the second private key as the encryption key; and

(h) coupling each encrypted hash value with its corresponding data packet.

14. A method for verifying digitally signed data in real time, the method comprising the steps of:

(a) processing the data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each packet of digitally signed data;

(b) verifying the contents of a first certificate issued by a certificate authority utilizing a public key issued by the certificate authority, the first certificate including a first public key of a long master key pair;

(c) verifying the contents of a second certificate issued by the sender of the data utilizing the first public key from the first certificate, the second certificate including a second public key of a short disposable key pair;

(d) decrypting the digital signature portion of the digitally signed data utilizing the second public key to obtain a second hash value; and

(e) comparing the first and second hash values.

15. A method for digitally signing data in real time, the method comprising the steps of:

(a) generating a disposable key pair, the disposable key pair including a short public key and a short private key;

(b) publishing the short public key;

(c) dividing the data to be signed into packets;

(d) for each packet of data, computing a hash value based on the data in that data packet utilizing a one way hashing function;

(e) encrypting the hash value utilizing the short private key; and

(f) coupling each encrypted hash value with its corresponding data packet.

16. A method for verifying digitally signed data in real time, the method comprising the steps of:

(a) processing the data portion of the digitally signed data through a one way hashing function to obtain a first hash value for each packet of digitally signed data;

(b) decrypting the digital signature portion of the digitally signed data utilizing a published short public key to obtain a second hash value; and

(c) comparing the first and second hash values.